Section 3.1 DCDS Security Overview

DCDS security is based on the establishment of User IDs and passwords and the assignment of functions, roles, and scopes. User IDs and passwords are used to limit system access and identify users, while functions, roles, and scopes are used to assign and control user capabilities. In general, functions represent a window or group of windows to which a user is granted access, while roles are a mechanism used to facilitate security administration by grouping related functions. Scope defines the breadth (e.g., statewide, a particular department, a particular agency, etc.) of the users' capabilities for particular functions.

Security Administrators

The Department of Management and Budget, Office of Financial Management (OFM) serves as the DCDS Statewide Security Administrator (SSA). The SSA is responsible for establishing statewide DCDS policies, procedures and forms; establishing and maintaining system default roles; and establishing and maintaining DCDS security for the DCDS Department Security Administrator (DSA) designated by each department's chief financial officer (CFO). The SSA defines the Department Security Administrators for each agency. Each agency is required to define additional users.

Department Security Administrators

DSAs are responsible for establishing and deleting DCDS User IDs and passwords for departmental users, insuring that users' capabilities are consistent with their duties, insuring that individual users are not assigned incompatible functions, monitoring users' access, and revoking or changing access as needed. DSAs may establish additional DCDS security administrators within the department, as needed, to assist with security administration.

Designating a DSA

The DSA is a critical position requiring a unique combination of skills, experience, authority, and integrity. In designating a DSA, CFOs should consider the following:

- Skills and Experience: To effectively perform his/her function, the DSA must possess a thorough knowledge of internal control concepts. In addition, he/she should have a working knowledge of DCDS, payroll processing, and labor distribution processing.

- Authority: The DSA must be at a level in the organization that allows him/her to perform his/her duties without undue interference or intimidation by higher levels in the organization.

- Integrity: The DSA has the ability to perform all DCDS functions. This represents a powerful capability, which, if misused, could result in fraudulent financial gain for the DSA or others. Therefore, it is extremely important that the DSA be trustworthy.

- Coordination with Other Departmental Security Administrators: DCDS security is closely related to the Human Resource Management Network (HRMN) security. To a lesser extent, it is also related to MAIN FACS security. At a minimum, the DSA must be aware of the need to coordinate his/her activities with other security administrators within the department. To eliminate or minimize the potential for miscommunication, the CFO may want to consider combining some or all of the security administration functions within a single individual or organizational unit.

To designate a DSA, departments must submit to OFM a completed *DCDS Security Request, Type 1 - Designation of DCDS Department Security Administrator*. For detailed procedures regarding completion and processing of this form, see Section 3.1.1.

Establishing Additional Security Administrators

If necessary to insure effective and efficient DCDS security administration, the DSA may establish additional security administrators within the department. At the time the DSA is designated, the DSA and CFO should consult regarding the need for additional security administrators. If additional security administrators are deemed necessary, the DSA should prepare internal departmental policies and procedures regarding the establishment of additional security administrators for approval by the CFO.

Additional DSAs must be established using the *Type l - Designation of DCDS Department Security Administrator* request form and submit it to the Department of Management and Budget, Office of Financial Management. The Type 1 form is also used when Agencies want to give update capabilities to the functions Define User (to add or delete users) and/or Generate Password (to reset passwords for users). The form should be signed by the Department Security Administrator and then submitted to DMB, OFM.

Assigning User IDs

In DCDS, the user ID is a 30 character, free-form field which must be unique within DCDS. If a security administrator attempts to enter a duplicate user ID, an error message (10075 - Duplicate Data) will be displayed.

To insure statewide uniformity and consistency, security administrators should use the user's GroupWise ID as the DCDS user ID, whenever possible. (Agencies may access the GroupWise User ID address list on the CNOC web page to verify the GroupWise ID assigned).

If the user does not have a GroupWise ID or the user's GroupWise ID is rejected in DCDS as a duplicate, the security administrator must assign a DCDS User ID consisting of the user's last name, first initial, and (if necessary to avoid duplicates in DCDS and/or GroupWise) a sequential number. Examples of valid User IDs for an employee named John Doe are "DoeJ", "DoeJ1", "DoeJ2", etc. When assigning user IDs, security administrators should verify that the assigned DCDS User ID does not already exist as a GroupWise ID. To ensure that the user ID is not used for a different GroupWise user in the future, they should also request that the statewide GroupWise administrator reserve the ID in GroupWise.

Assigning User Capabilities

Security administrators establish user capabilities by assigning the appropriate system default roles or developing and assigning appropriate internal departmental roles. In assigning user capabilities, security administrators (both DSAs and additional security administrators) should consider the following:

> User's Duties: The assigned functions, roles, and scopes should be consistent with the user's current duties.
>
> Internal Control: The assigned functions, roles, and scopes should not create an unacceptable internal control risk because of incompatible capabilities in DCDS or other systems.

Assignment of user capabilities must be documented. The department may use the *DCDS Security Request, Type 2 - Agency Roles and Functions* to assign user capabilities. For detailed procedures regarding completion and processing of this form, see Section 3.1.1
A department may also develop its own internal forms for this purpose, however, it must meet the following minimum standards:

- Completion of the information included in the 'User Information' section of the statewide form;
- A signed user agreement that includes language identical to that on the statewide form;
- Approval by both the user's supervisor and the DSA that includes language identical to that on the statewide form; and
- Documentation of the date entered in DCDS and the signature of the individual who entered the information into DCDS.

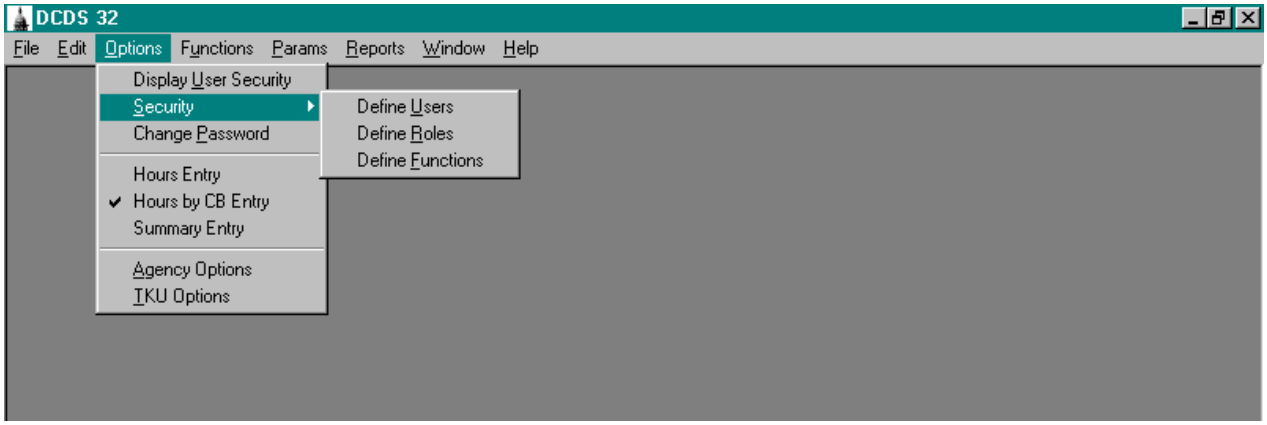
DCDS Security Windows

The security functionality of DCDS consists of the following windows accessed through the Options menu:

- Display User Security
- Security (Define Users, Define Roles, Define Functions)
- Change Password

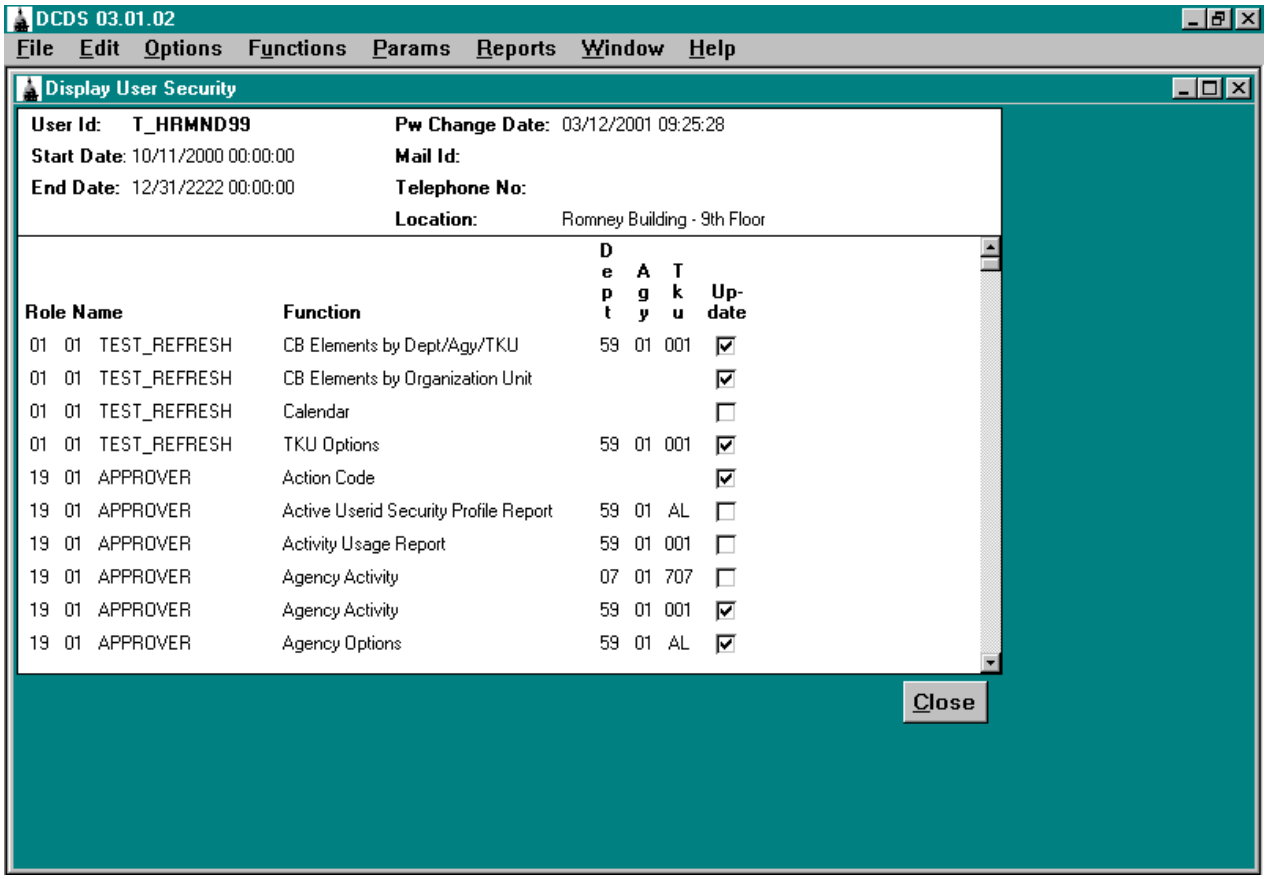
The Security windows are accessed through the Options, Security, Define Users, Roles or Functions menu items on the menu bar.

Each window consists of a Selection tab which is displayed first. The Selection Criteria window is provided to enter known criteria to narrow in on specific users. The Selection List window displays data that matches the Selection Criteria. Once a user is selected, any of the other tabs can be accessed.

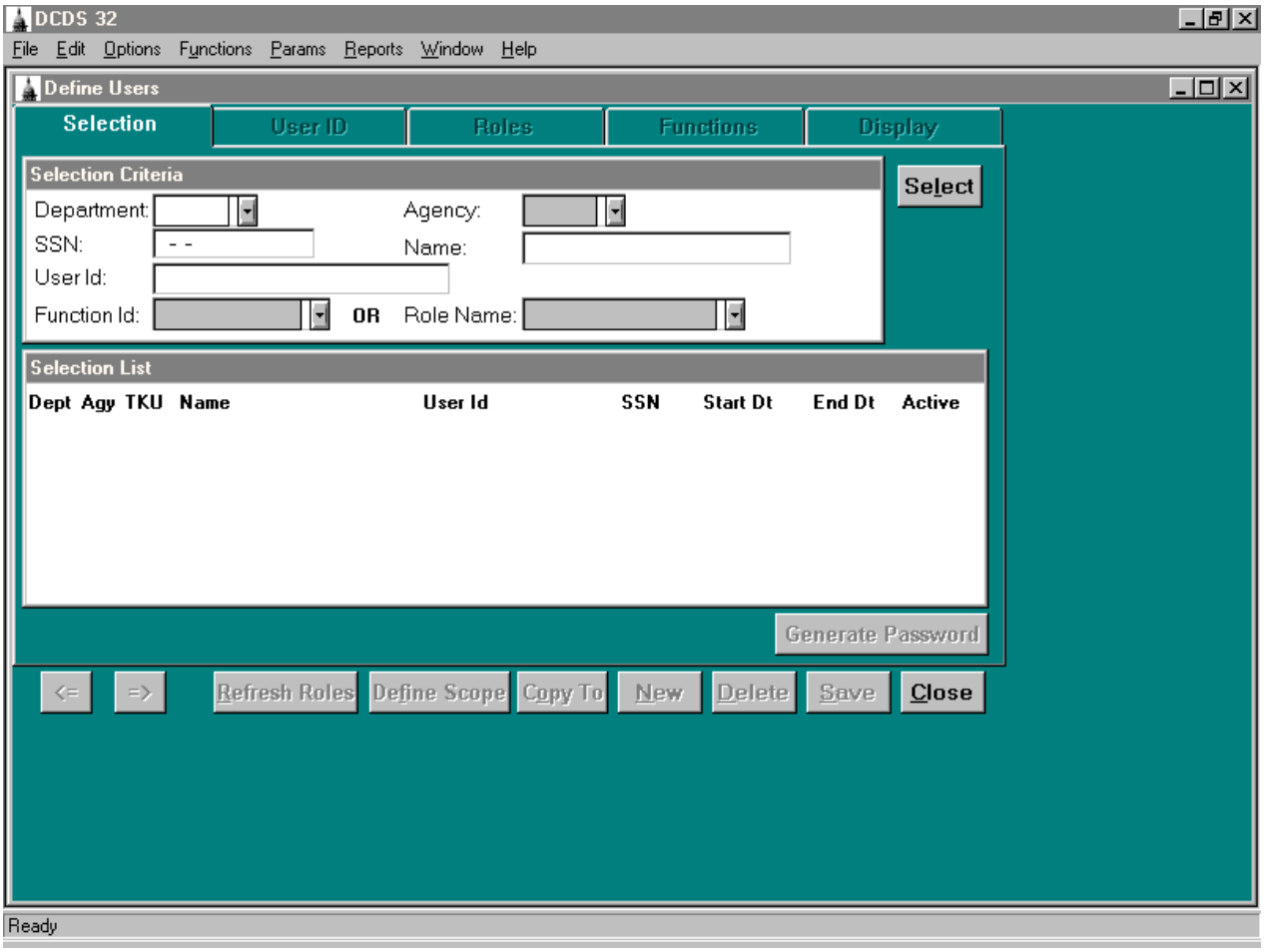


Following is a description and sample of each window.

Display User Security - The Display User window is an inquiry which displays a person's levels of security (see Section 3.2 for details).

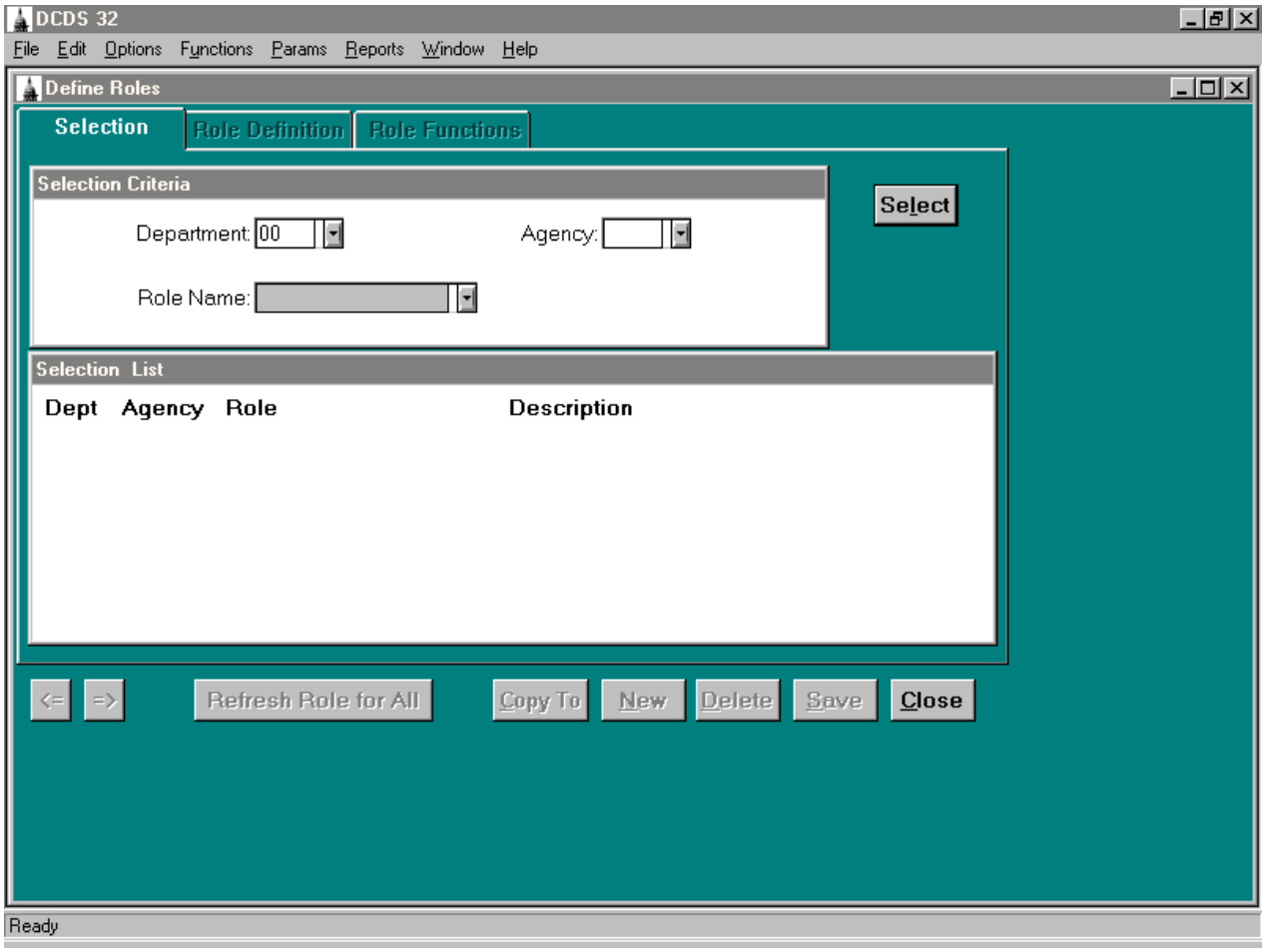


- **Security (Define Users, Define Roles, Define Functions)**
  - **Define Users** - The Define Users window is used to create User IDs and define access for users. The functions accessed through the Define Users window include defining, copying, updating or deleting users' access; generating temporary passwords; adding and/or removing roles; defining the scope of functions (statewide, department, agency, TKU etc.), and viewing detail security information (see Sections 3.3-3.3.4 for details). This window consists of the following tabs:
    - Selection
    - User ID
    - Roles
    - Functions
    - Display



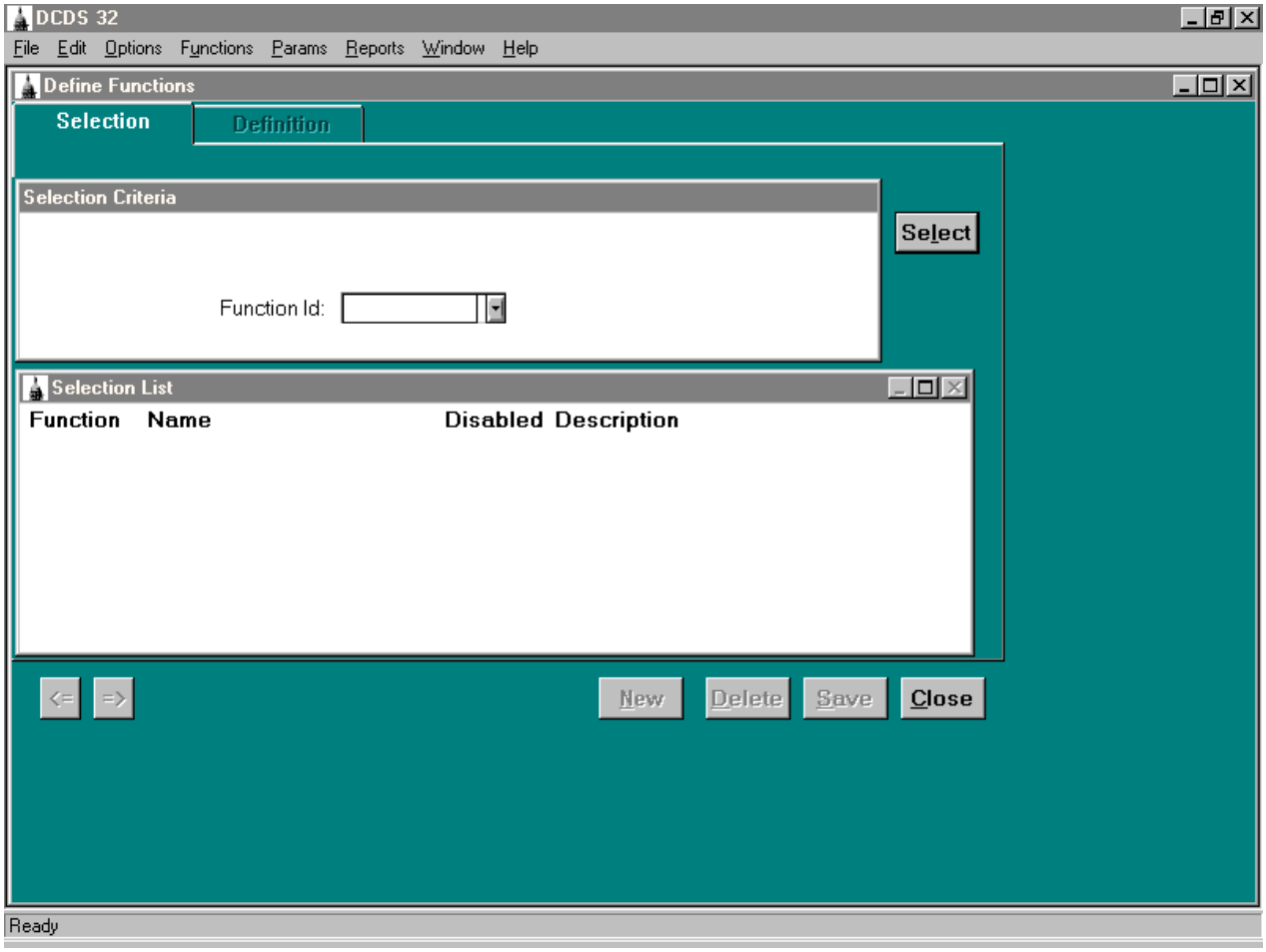
- **Define Roles** - The Define Roles window is used to add, copy and update/delete roles for users of DCDS. Roles are a mechanism used to facilitate security administration by grouping related functions. Agencies may use statewide default roles or create their own roles. Examples of roles are Individual Time Entry, Data Collection, and Timekeeper (see Section 3.4 for details). This window consists of the following tabs:

  - Selection
  - Role Definition
  - Role Function



- **Define Functions** - The Define Functions window allows the Statewide Security Administrator to define functions that the DSAs will use to assign roles. Functions define the actions which can be performed by a user. In general, functions represent a window or group of windows to which a user is granted access. Examples of functions are Data Collection - Time, TA Inquiry - Time, and Payroll Distribution by CB Report (see Section 3.5 for details). This window consists of the following tabs:

  - Selection
  - Definition



- Change Password - The Change Password window allows a user to change their own password to access DCDS (see Section 3.3 for details).